タイトル	An encryption technique by digital holography
著者	Takai, Nobukatsu
引用	工学研究 : 北海学園大学大学院工学研究科紀要(11): 47-54
発行日	2011-09-30

研究論文

An encryption technique by digital holography

Nobukatsu Takai*

Abstract

A diffuse-type digital holography obeying to the theory of optical holography is applied for cryptography in which a plain text is encrypted. The technique of cryptography is based on a fact that the error of the image reconstructed from the 8 bits digital hologram is smaller than 0 bit in a sense of statistics. The cryptography of the plain text using a digital holography and a recovering algorithm is proposed. In this study, the diffuse-type hologram plays the role of the encrypted medium of the plain text. An algorithm by which the reconstruction error of digital holography is removed in a complete form still without a single bit error is proposed. An idea of the key for protecting the plain text recovered from the digital hologram is also presented.

1. Introduction

Optical holography[1,2] is a technique by which both the amplitude and the phase of an optical wave from an object are recorded on a hologram. If it emits diffusion light by the random phase modulation on its surface, the hologram intensity is in stochastic process, and becomes a uniform distribution as a whole. Nevertheless, we can recover both the amplitude and the phase of the object and, as a result, can obtain the reconstruction image. In this way the optical hologram may be regarded as a kind of the encrypted media in a sense that they have whole information of the object in a random fashion.

Digital holography is a technique originally based on the optical holography mentioned above and is executed in a computer. This technique is usually applied for digital images, and the information is recorded on a digital hologram. The image reconstructed from the digital hologram looks at least visually being the same as that of the original one. However, as will be seen, it has some errors derived from random phase modulation together with quantization errors in digital signal processing. Since such errors are never avoided in the digital holography, its applications are limited to the field of digital signal (image) processing where images are evaluated by vision.

In the present study, the procedure by which the diffuse-type Fourier transform digital hologram is constructed and the image is reconstructed from it is described briefly first. Then, the experiments are conducted in a computer for images consisting of 8 bits data format. The error of the reconstruction image is quantitatively investigated in terms of the standard deviation of the image difference between the original and reconstructed images. It is shown that the reconstruction error occurs in the bit plane smaller than 0 bit when the standard deviation of the random phase used for constructing the diffuse-type hologram is larger approximately than $\pi/2$.

The algorithm which completely removes a reconstruction error is presented under the conditions that such an error is small, and its

* 北海学園大学大学院工学研究科電子情報工学専攻
Graduate School of Engineering (Electronics and Information Eng.), Hokkai-Gakuen University

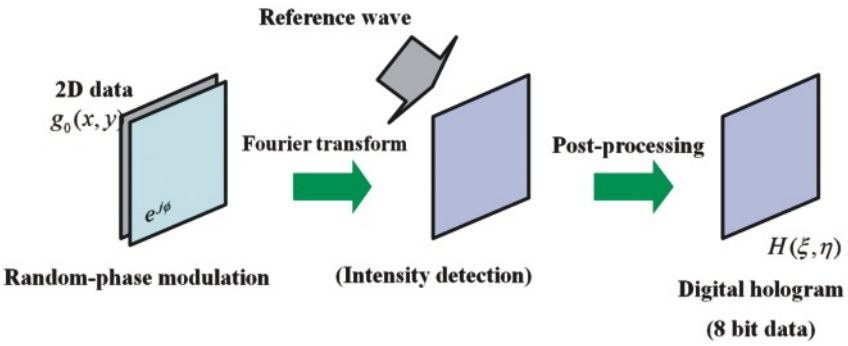


Fig.1 Schematic view of the procedure which constructs diffuse-type Fourier transform digital holograms.

validity is certainly verified experimentally. This success leads us to apply the digital holography to any digital content, for example numerical data, text documents and others. Really, it will be seen in this article that a text document is treated in digital holography, and it is shown that the digital hologram plays the role of a cryptogram of the plain text. Finally, it is described that a way embedding the encryption/decryption keys for security in the digital holograms is easily performed.

2. Diffuse-type Fourier transform digital holography

The mathematical description of the diffuse-type Fourier transform digital holography was already given by the author in detail.[3] In this point, only the procedure which constructs the hologram and then reconstructs the image from it is briefly described by the help of Fig.1. In the figure, an original data (i.e., digital content) is expressed by $g_0(x,y)$ which denotes the two-dimensional pixel array such as images and takes non-negative values. First, in order to construct the diffuse-type hologram, the data $g_0(x,y)$ is modulated by random phase $\phi(x,y)$. Actually, all the pixel data are multiplied by the complex values of $\exp(i\phi)$, ϕ being given by Gaussian random numbers with zero mean. As is shown in Fig. 1, the randomly phase-modulated data is Fourier transformed and, then, the interference intensity between the Fourier transformed data and a reference signal wave which is given by a plane wave with inclination is calculated. In digital holography, as a post-processing, the components which do not concern the reconstruction are removed by substituting non-interference terms, and we finally obtain the digital holograms of the two-dimensional data.

At the reconstruction stage of objects, the reconstruction plane wave is multiplied to the digital hologram and the inverse-Fourier transform of the resultant signal is calculated. In this way we can obtain the reconstruction images. In this stage, if the reconstruction wave with the amplitude of unity and the phase of zero is chosen, the reconstruction image is easily obtained only by executing the inverse-Fourier transform of the digital hologram.

An example of a digital hologram and its reconstruction image is shown in Fig.2 together with the original one. In this case, the size of the whole field is 512×512, and that of the content image is 256×256. As is seen in the figure, two reconstruction images, corresponding to the real and the imaginary ones in optical holography, appear symmetrically with respect to the center of the origin. The locations of two reconstruction images are adjustable by the inclination parameters relating to the reference wave. It is particularly important that the reconstruction images are obtained independently of the random phase modulation used in the stage of constructing the hologram.

It may be seen in Fig.2 that the reconstruc-

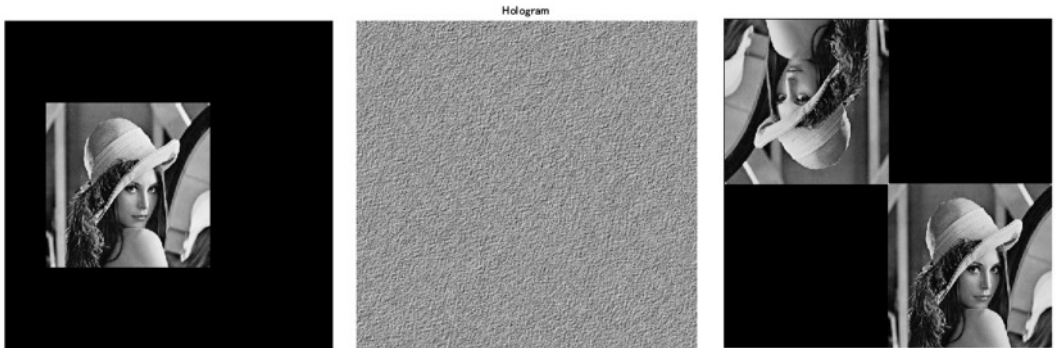


Fig.2 Original image (left), hologram (center) and reconstruction images (right).

tion images are in beautiful agreement with the original one at a glance. In practice, however, some errors are contained in the reconstruction images. In such error evaluation, it is noted that the data of the digital hologram must be 8 bits in data format according to the standard format for images, even if it is constructed with 16 bits double precisions. The transformation from 16 to 8 bits of hologram data results in the error coming from the 8 bits quantization, and we have to be always careful to this error in treating the 8 bits digital hologram.

3. Digital holography of the document text

The subject of the present study is to apply the technique of digital holography for the document text. To say nothing, all the data based on a computer, e.g., image, text, music and so on, is treated in numerical arrangement. Therefore, not only the image but also the document text can be treated as an object in digital holography by expressing it as two-dimensional array data. In this study, the plain text of Fig.3 consisting of 950 ASCII characters including spaces was used in the experiments and treated as an array of the size 15×64. That is, in place of the image data such as Fig.2, the numerical array of the plain text was treated as the text-image data consisting of the values 0 to 127 in decimal which expresses the ASCII characters given by 7 bits.

The image of the text, its digital hologram, and the reconstruction image obtained in the experiment are shown in Fig.4. In this case,

abc =

A holographic technique is applied for digital watermarking by a computer. A digital-watermark image to be hidden is phase modulated in a random fashion, and its Fourier-transformed hologram is superposed on a content image. The watermark is reconstructed by means of holographic-reconstruction technique from the bit-map image that hides it. In the study the processes of constructing and reconstructing a digital hologram are described on a basis of the theory of Fourier Optics. The conditions for superposing the hologram onto the content images are investigated in detail. The validity of the present method is verified by changing the weighting of the hologram relative to that of the content image. The effect of image size is also discussed with respect to reconstruction of the watermark, and it is shown that watermark information in a form of a diffuse-type Fourier-transform hologram cannot be removed by cutting it out of the host image.

Fig.3 The content data of the plain text used in experiments. abc is the name of a variable of this data.

the text image and the reconstruction one occupy a rectangular area with 15×64 pixels, and have the brightness distribution corresponding to the value of the character codes. If the reconstruction image were in complete agreement with the original one, the content of the plain text can be correctly obtained by decoding it. However, as is seen in Fig.5 which is the content of the plain text from the reconstruction image is quite different from the original one. In this way, the errors of reconstruction are obviously found out in the reconstructed plain text, even if the reconstructed image pattern is visually resemble to the original one.

4. Error evaluation of reconstruction images

The pixel values of the reconstruction

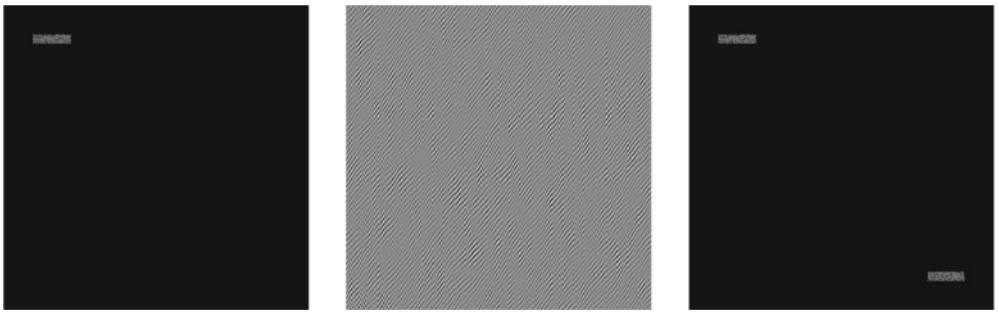
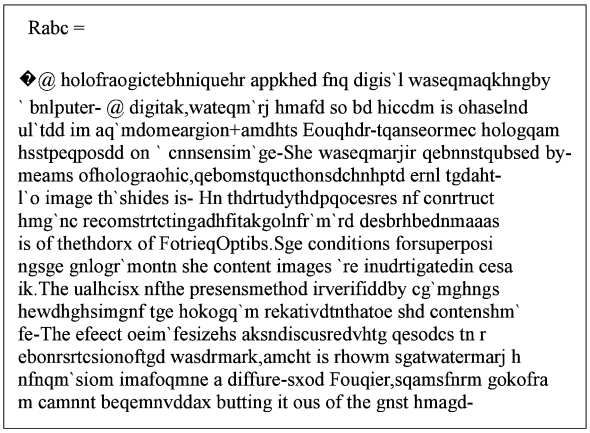


Fig.4 Original text-image (left), its hologram (center) and the reconstructed text-images (right). The number of characters is 950 including spaces, and the size of the text image data is 15×64 pixels.

Rabc =



```
 Rabc =

 ?@ holofraogictebhniquehr appkhed fnq digis`l waseqmaqkhngby
 ` bnlputer- @ digitak,wateqm`rj hmafd so bd hiccdm is ohaselnd
 ul`tdd im aq`mdomeargion+amdhts Eouqhdr-tqanseormec hologqam
 hsstpeqposdd on ` cnnsensim`ge-She waseqmarjir qebnnstqubsed by-
 meams ofholograohic,qebomstqucthonsdchnhptd ernl tgdaht-
 l`o image th`shides is- Hn thdrtudythdpqocesres nf conrtruct
 hmg`nc recomstrtctingadhfitakgolnfr`m`rd desbrhbednmaaas
 is of thethdorx of FotrieqOptibs.Sge conditions forsuperposi
 ngsge gnlogr`montn she content images `re inudrtigatedin cesa
 ik.The ualhcisx nfthe presensmethod irverifiddby cg`mghngs
 hewdhghsimgnf tge hokogq`m rekativdtnthatoe shd contenshm`
 fe-The efeect oeim`fesizehs aksndiscusredvhtg qesodcs tn r
 ebonrsrtcsionoftgd wasdrmark,amcht is rhowm sgatwatermarj h
 nfnqm`siom imafoqmne a diffure-sxod Fouqier,sqamsfnrm gokofra
 m camnnt beqemnvddax butting it ous of the gnst hmagd-
```

Fig. 5 An example of the content of the plain text obtained straightforwardly from the reconstruction image. Rabc is the name of a variable expressing the reconstruction image.

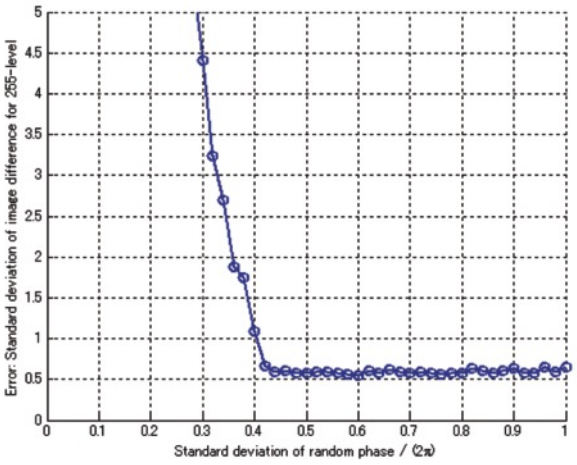


Fig.6 Experimental result of the standard deviation of the reconstruction error defined by Eq.(1) as a function of the standard deviation of the random phase.

image $I_{reconstructed}$ (either one of reconstruction images) and those of the original one $I_{original}$ were compared and the statistical error has been evaluated numerically. To do this, the standard deviation of the difference $\Delta I = I_{reconstructed} - I_{original}$, i.e.,

$$\sigma_{\Delta I} = \sqrt{\langle \Delta I^2 \rangle} \tag{1}$$

has been used as an evaluation parameter of the reconstruction error, $\langle \ldots \rangle$ denoting the ensemble average.

Figure 6 is the experimental result of the standard deviation, defined by Eq.(1), as a function of $\sigma_p/2\pi$, σ_p being the standard deviation of the random phase used at the stage of hologram construction. It is recognized in the figure that the reconstruction error takes a large value in the region of approximately $\sigma_p < \pi$, steeply decreases with an increase of σ_p, and finally takes an almost constant value beyond $\sigma_p \sim \pi$.

The behavior of the reconstruction error in the region of small value of σ_p comes from the error due to 8 bits quantization of holograms. The reason why it takes large values in that region can be explained as follows. That is, when the variation of the random phase is so gentle and then σ_p is small, the almost power of the spectrum in the Fourier transform plane distributes in the low frequency region and the strong spectral peak usually appears around the origin in the spectral space. In such a situation, the 8 bits quantization of the hologram intensity is not appropriate because the

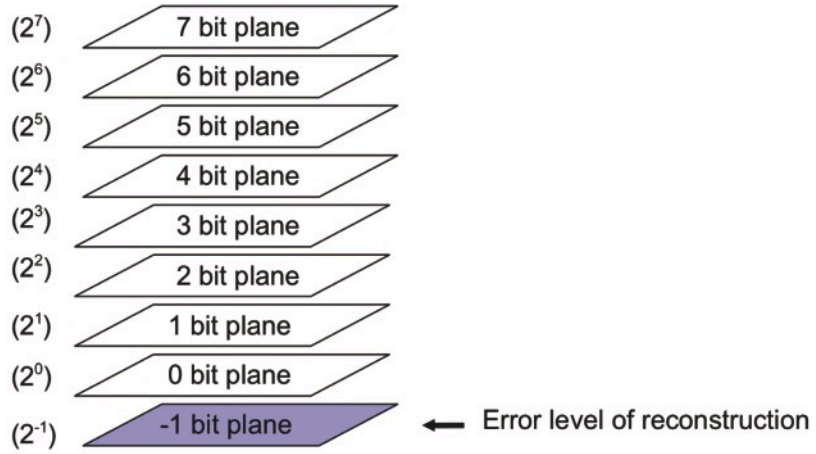


Fig.7 Error level of the reconstruction image in bit-planes when $\sigma_p \geq \pi$.

higher frequency components consisting of small values are ignored in effect, and the reconstruction error becomes large.

On the other hand, when the random phase variation is violent, the spectrum distributes homogenously in the spectral region as a whole. For such a homogenous hologram, the 8 bits quantization is expected to be performed successfully for all spectral components. As a result, the reconstruction error becomes fairly small. In this way, in order for digital holograms to be well constructed, it is necessary for the random phase modulus to be approximately $\sigma_p \geq \pi$ in the stage of hologram construction.

In the experiment, the minimum and the maximum of the reconstruction image as well as the hologram were normalized to be 0 and 255, respectively. For such full dynamic range data of 8 bits, the error of the reconstruction image derived from the well-constructed hologram was obtained to be approximately 0.6 in terms of standard deviation for 255 gray levels (see Fig.6). The bit-plane level of this error is shown as "erorr level of reconstruction" in Fig. 7 to be located in the position less than the 0 bit plane. Although the reconstruction error is fairly small, it is noted that the complete reconstruction of the digital content is never achieved in digital holography. Therefore, a complete way to remove the error is required in order to recover correctly the digital content.

5. Algorithm fully recovering the digital content

The error level indicated in the bit-planes of Fig.7 is worthwhile to find out a means for completely recovering the digital content. This figure indicates that the error level of the reconstruction image is less than 0 bit plane under the condition of $\sigma_p \geq \pi$. Therefore, the error affecting the 3 bits plane does never occur in practice because the error in the 3 bits plane is more than approximately ten times the reconstruction error (i.e., approximately 0.6) in terms of the standard deviation. Based on this fact, the following algorithm by which the digital content is recovered in a complete form was found.

This algorithm is able to completely recover the original digital content of 8 bits data from the reconstruction image with small errors. The procedure of the algorithm consists of following four steps and is schematically shown in Fig.8, in which only five data of 8 bits is used as a concrete example to help understanding of it. Each step of the algorithm presented here is explained as follows.

1st step: The 8 bits data at a pixel of the original content-image is divided into two parts, the upper 4 and the lower 4 bits.

2nd step: A pair of 8 bits data is newly made from two 4 bits data divided in the 1st step in a way that each 4 bits are placed at the position

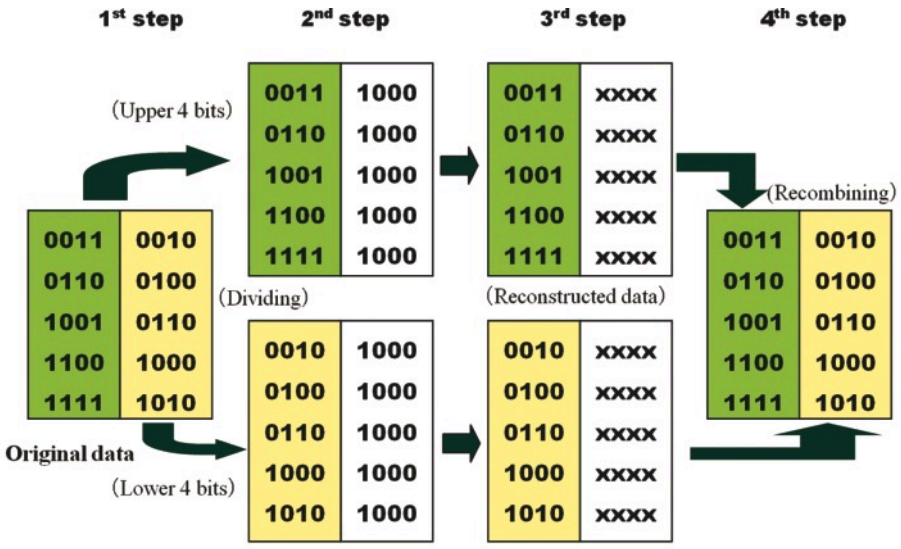


Fig.8 Schematic diagram for explaining the algorithm completely recovering the original data from the reconstruction data with small error.

of the upper 4 bits, and (1000) are placed at that of the lower 4 bits for every data. Then, we determine the configuration of the array consisting of a pair of 8 bits data, and make a digital hologram of the resultant array.

3rd step: We get the reconstruction image from the hologram of the array constructed in the 2nd step. Then, we pick up only the upper 4 bits of the reconstruction data, and discard all the lower 4 bits (the parts of (xxxx) in Fig. 8).

4th step: Finally, two upper 4 bits obtained in the 3rd step are recombined according to the configuration determined in the 2nd step.

Executing the above algorithm, the digital content is obtained in a complete form from the reconstruction image with small error because both the upper and lower 4 bits of the original content are treated as the upper 4 bits of the 8 bits data newly constructed. In the procedure, the 2nd step in which the lower 4 bits of every data are placed as (1000) is especially important. By this processing, the reconstruction error within the extent of -8 to +7 in decimal does not affect to the upper 4 bits, even if the reconstruction image contains some accounts of the error. In other words, the error of the reconstruction image is successfully absorbed to that extent. As a result, the upper 4 bits of both data divided are obtained without suffering any error, so that recombining them gives us the original data in a perfect form.

Rabc =

A holographic technique is applied for digital watermarking by a computer. A digital-watermark image to be hidden is phase modulated in a random fashion, and its Fourier-transformed hologram is superposed on a content image. The watermark is reconstructed by means of holographic-reconstruction technique from the bit-map image that hides it. In the study the processes of constructing and reconstructing a digital hologram are described on a basis of the theory of Fourier Optics. The conditions for superposing the hologram onto the content images are investigated in detail. The validity of the present method is verified by changing the weighting of the hologram relative to that of the content image. The effect of image size is also discussed with respect to reconstruction of the watermark, and it is shown that watermark information in a form of a diffuse-type Fourier-transform hologram cannot be removed by cutting it out of the host image.

Fig.9 The plain text recovered in a complete form. This is obtained from the reconstruction image by applying the recovering algorithm presented and is named as Rabc.

The validity of the algorithm presented here has been verified for the plain text of Fig. 3. By applying the present algorithm, although the reconstruction image surely contains unavoidable errors mentioned previously, the perfect plain text has been recovered from it and is shown in Fig.9.

It should be emphasized here that the details of the data of the reconstruction image as well as those of the hologram are different

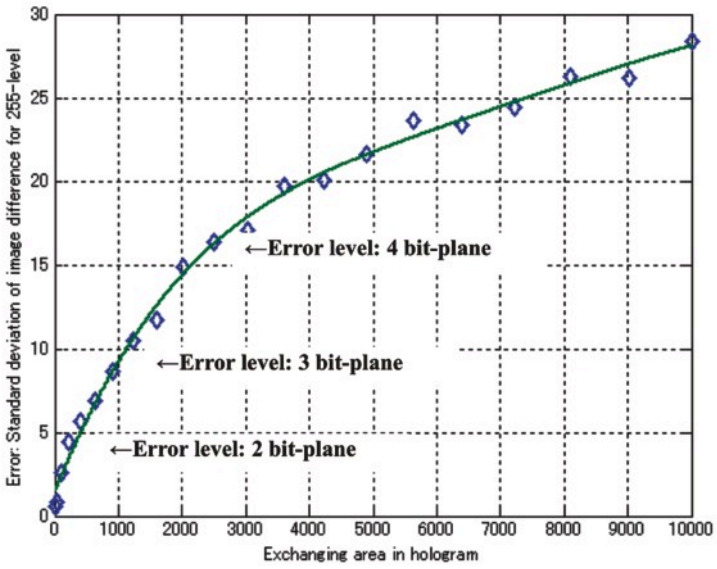


Fig.10 The reconstruction error when two block areas in the digital hologram are exchanged in position with each other. The horizontal axis is the area of the exchanging square blocks in pixels.

whenever we repeat the experiments. This comes from a fact that the content of the random numbers used to make the diffuse-type holograms is updated each time by different ones. Nevertheless, we can certainly recover the correct plain text in the repeated experiments.

6. Holographic cryptography with respect to the plain text

Using the recovering algorithm in digital holography described above, the plain text can be encrypted in a form of the diffuse-type digital hologram and decrypted correctly from it. As was seen in Fig.3, the pixel values of the diffuse-type Fourier transform hologram are quite random because it is constructed by using the random phase modulation. In this way, such a hologram may be regarded as one of media of encrypting the plain text.

We are now in a position to describe the holographic cryptography by digital holography. In general, a cryptogram is made by encrypting a plain text with the help of a encryption key, and the plain text is recovered by decrypting the cryptogram with the help of the same key.[4–6] To do this in the holographic cryptography, the new concept of the key of cryptography is required for encryption/decryption. In this point, it should be noted that the recovering algorithm is based on the small-error reconstruction image from the hologram. If the error level of the reconstruction image is larger than the 3 bit-planes, the recovering algorithm becomes invalid in principle, and the original plain text can be never recovered. The cryptography key can be introduced to the digital hologram by realizing the situation that the recovering algorithm becomes invalid by some way.

We can show an example of such a cryptography key. A digital hologram contains all the information with respect to the digital content, and gives us the reconstruction image with small error. It was found, however, that the reconstruction error greatly increases by changing the configuration of parts inside the hologram. For example, considering the two blocks in the hologram with the same shape and exchanging them each other increase greatly the reconstruction error. This error dependence on the size of the block area was investigated by exchanging of square blocks in the digital hologram, and its result is shown in Fig.10.

As is seen in the figure, the reconstruction error greatly increases with an increase of the area of exchanging blocks. As a result, it was found that the choice of two exchanging blocks with the size (or area) for which the reconstruction error is larger than the 3 bit level makes the recovering algorithm quite invalid. This fact was verified repeatedly in the experiments with respect to the encryption of the plain text shown in the previous section. Furthermore, it was found that the error level larger than not only the 3 bit-plane but also the 2 bit-plane makes the recovering algorithm invalid. This may come from the fact that the error level is given by the standard deviation. Thus, it seems that the actual errors occur approximately at the 2-bit plane or more.

In this way, exchanging two blocks inside a hologram plays the role of a encryption key of the hologram. To put it concretely when the rectangular blocks are used, the coordinates, (x_1,y_1) and (x_2,y_2) of each exchanging block and the lengths (l_x,l_y) of its sides can be used as key parameters. The encryption is performed by exchanging blocks using these key parameters, and the decryption can do only by a person who knows them secretly, because he can put the hologram configuration back in its place, and recover the plain text with the help of the recovering algorithm.

7. Concluding remarks

In this study, the error level of the reconstruction image from digital hologram has been investigated numerically. It has been found that the error level is in a place smaller than a 0 bit-plane in terms of the standard deviation, when the random phase modulation is applied to the object (i.e., digital content) in the stage of hologram construction under the condition of approximately $\sigma_p \geq \pi$, σ_p being the standard deviation of the random phase. On the basis of this fact, the algorithm by which the reconstruction error is removed in a complete form has been presented.

Furthermore, a novel cryptography of the plain text by using digital holography and the recovering algorithm is proposed. In this cryptography, the diffuse-type hologram plays the role of the encrypted medium of the plain text. It has been shown that the hologram is locked by exchanging the two parts inside it.

The validity of the method presented has been verified for the English plain text. The treatment for the Japanese plain text in which characters are coded in a form of 16 bits is slightly different from English one. In the case of Japanese plain text, a character of 16 bits is divided beforehand into two 8 bits codes, and the identical recovering algorithm is applied for the divided 8 bits. By this procedure, the author has succeeded completely recovering the Japanese plain text from the digital hologram.

This research has been supported by the subsidy to the Hi-Tech Research Center, Hokkai-Gakuen University.

References

1 M. Born and E. Wolf: *Priciples of Optics*, Chpt.8, 412–516 (Cambridge University Press, 7th ed. 1999).
2 J. W. Goodman: *Fourier Optics*, Chp.8, 198–254 (McGraw-Hill, San Francisco, 1968).
3 N. Takai and Y. Mifune: Digital watermarking by a holographic technique, Applied Optics, Vol.41, No.5, 865–873 (2002).
4 B. Schneier; *Applied Cryptography: Protocols, Algrithms, and Source Code in C*; 2nd ed. (John Wiley & Sons Inc. 1995).
5 S. Flannery and D. Flannery: *In Code: A mathematical Journey* (Algonquin Books of Chapel Hill., 2002).
6 S. Singh: *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography* (Anchor, 2000).